安全な取引方法

安全取引のために, 以下のことに注意する:

USER ID, PASSWORD, MPIN, トークン

1. J NET Business & J MOBILE Password は, 他人には知りにくいユニークな組み合わせで定期的に変更する。
2. 銀行員を含む他者には、自分のパスワードや PIN を渡さない。
3. J NET BUSINESS & J MOBILE のパスワードをコンピュータ/ノートパソコン, スマートフォン, コンピュータに保存しない。
4. 電子メールで機密情報を送信しない。なお, Jトラスト銀行では, 電子メールなど無担保の電子的手段による機密情報の請求は行わないこととしている。
5. 銀行から送られてくる取引通知に常に注意を払い、実行された取引の価値を確認する。

コンピュータ/ノートパソコン, スマートフォン/タブレット端末

1. 信頼されるパソコンやネットワークを利用して、J NET Business & J MOBILE のサービスをご利用いただける。例えば、インターネットカフェや信頼できないネットワークでは、カフェやショッピングセンター内のショップが提供する wifi アクセスポイントなど、パブリックコンピュータの使用を避けることが最善である。
2. J NET BUSINESS & J MOBILE でお取引いただく Web ブラウザーやアプリのバージョンを更新/ 更新する。
3. 使用するコンピュータ/ノートブックがキーロガーデバイスから安全であることを確認する。
4. ウイルスやマルウェアが含まれているファイルは個人データを盗む可能性があるため、ダウンロードには注意する。
5. J NET BUSINESS & J MOBILE で取引する際に使用する機器から完全にログオフ。

ネットワーク/ネットワーク

J NET Business & J MOBILE でお取引の際は、公衆の Wi-Fi アクセスを利用しない。公衆に利用可能な無線ネットワークは, 犯罪者が携帯電話から情報を盗むためにも利用することができ、その一つが銀行情報である。

セーフゾーン

Jトラスト銀行が発行する公式申込書は、Jトラスト銀行の公式ウェブサイトにアクセスするか、申込書店から直接 Jトラスト銀行の申込書をダウンロードしてご利用ください。または、セーフゾーンにいるかどうかを知るには、'https' などの正しい URL から始める。また、モニター画面の右下角に, 参入しているウェブサイトが安全か否かを示すパドロックイメージが表示される。

検証

取引を行う前に, まず Jトラスト銀行にアクセスしていることを確認する。連絡先番号などの情報を確認し、エラーが発生した場合は住所をクリアする。また、ウェブサイトの住所から有効な口座番号まで、目標とする口座番号について電話で銀行に確認する。

更新

モバイルバンキングアプリケーションを更新し続ける、最新バージョンを手動で更新する、または自動更新機能を有効にする。J MOBILE サービスでは, 常に最新版のアプリケーションをご利用ください。

その他

1. J NET Business & J MOBILE を通じた取引の安全性に関して考慮すべき事項は以下の通りである:

a. フィッシング

フィッシングとは、利用者に損害を与えることができる利用者 ID、暗証番号等の顧客の機密情報を得ることを目的として、当行の公式サイトに非常に類似した偽造ウェブサイトを作成することにより特定の当事者が行う不正行為の手法である。フィッシングに対するセキュリティーは次のようにいくつかの方法で行うことができる:

1. J ネット, J ネットビジネスは, 下記のオフィシャルサイトの住所でご確認ください。
   https://jnet.jtrustbank.co.id/eb-personel (個人顧客向け) および http://jnetbusiness.jtrustbank.co.id/eb-business (法人顧客向け) またはウェブサイト www.jtrustbank.co.id で利用可能なリンクを使用する. ウェブサイト名のスペルを常にダブルチェックするので, 記号の使用を含めてタイプはない.
2. ショートカットとブックマークを使用できるように、ショートカットを作成するかまたは J TRUST NET 個別サイトアドレスをブラウザ(ブックマーク)に保存する。
   J TRUST NET 個別サイトアドレスの入力エラーを最小限に抑える。
3. J トラスト銀行役員の名義で, 暗証番号を含む個人情報の提供を求める電話、ファックス、電子メールを通じて行動する個人からの不正な試みに対して警告を発する。
   J トラスト銀行では, ご利用の暗証番号・暗証番号のご請求・ご請求しない。
4. 自動で開く(ポップアップされる)ウェブページや, ウェブサイトのデジタル広告/バナーなどの疑わしいリンクから, 決してユーザーID とパスワードを入力しない。

b. ウイルス

ウイルスとは, 感染したコンピュータ上の OS, アプリケーション、データを傷つけるために、特定の目的で作成されたコンピュータソフトウェアのことである。ウイルスは, 電子メール、CD、リムーバブルストレージ、インターネットやネットワークからダウンロードしたプログラム, 安全でないウェブサイトのページなど, 多くの媒体を介して伝播することがある。ウィルス感染の影響の例としては、コンピュータデバイスが不安定になり、しばしば「ハング」(凍結)したり, データが削除されたり, 一部のアプリケーションプログラムが適切に機能しなくなったりすることがある。ウィルスに対する防御は, 次のようにいくつかの方法で行うことができる:

1. 最新のアンチウイルスを使用して, コンピュータがウィルス, マルウェア, スパイウェア, またはその他のアプリケーションに感染することを防ぐ。
2. メール添付文書は, 機密データを盗み出す可能性のあるウィルスを含む可能性があるため, 注意してダウンロードする。添付を開ける前に,、まずウイルス対策ソフトを使ってスキャンする。
3. ソフトウェアのダウンロードやインストールには注意する。
4. リムーバブルストレージデバイスをコンピュータに接続する際には注意する。アンチウイルスソフトウェアを使用して, リムーバブルストレージをスキャンしてから, コンテンツを開く。
5. 信用できないウェブアドレスからのアクセスやファイルのダウンロードを避ける。

c. スパイウェア

スパイウェアは、クレジットカード番号, ユーザーID, PIN/Password, 口座番号, メールアドレスなどの重要な個人情報を, 感染したコンピュータデバイスから検索するために作成されたコンピュータソフトウェアで、第三者の利益のためにこれらの情報を特定の場所に送信する。スパイウェアは, メール添付や危険なソース/ウェブサイトからインストールされたプログラムを介してインストールすることができる。スパイウェアを拡散するためにウイルスをプログラムすることもできる。スパイウェアが機能する方法は, 検出が難しい傾向があるため, 作成者/スプレッダーが望む情報を収集しやすくなる。スパイウェアに対するセキュリティは, ウイルスに対するセキュリティと同じである。

2. セキュリティ証明書と https://jnet.jtrustbank.co.id/eb-personel(個人顧客向け)および http://jnetbusiness.jtrustbank.co.id/eb-business(法人顧客向け)のウェブサイトアドレスの詳細を確認するには, 使用しているブラウザのウェブアドレスの隣にある緑のバー/セキュリティのマークで証明書を表示するを選択する。
   J NET, J NET BUSINESS へのアクセス時に証明書に関する警告メッセージが表示される場合は, Web サイトへのアクセスや, 入力した Web サイト名をダブルチェックしない.
3. インターネットブラウザに, 現在アクセスしているページがセキュリティコンセプトレイヤー(SSL)を使用して暗号化されていることを示すパドロック/キーイメージがあることを確認する。ロック/キーイメージが表示されない場合は, ログアウトする。
4. J TRUST NET Individual に対して, 電話等を通じた誰かの依頼により, 何らかの理由により, 報奨金等を受領した場合は, 登録しない。J トラスト銀行電子銀行サービスの正式登録は, 支店または J トラスト銀行電子銀行ポータルを通じてのみ行う。
5. これを行ったことがない間に, J トラスト銀行から口座の活動に関する通知があった場合, 直ちに最寄りの J トラスト銀行支店または J トラスト銀行コールセンターを訪問し, フォローアップを行う。
6. 不審な請求があった場合は, J トラストコールセンター「Ask J」を通じて J トラスト銀行に 1500615 で確認する.
7. コンピュータ/ノートパソコン, スマートフォン/タブレット, ウェブページ/アプリケーションにアクセスされていることについて, 奇妙/異常なことがあると感じた場合は, 取引活動を停止する.